

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS**

MICHAEL SMITH, individually and on behalf of his minor children J.S., B.S., T.S., and B.S., and TUSSIE SMITH, individually and on behalf of her minor children J.S., B.S., T.S., and B.S., and on behalf of all others similarly situated,

Plaintiffs,

v.

ESO SOLUTIONS, INC. and BON  
SECOURS MERCY HEALTH, INC., d/b/a  
MERCY HEALTH,

Defendants.

Case No. 1:24-cv-00003

CLASS ACTION

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT**

Plaintiffs Michael Smith and Tussie Smith (together, “Plaintiffs”), individually, on behalf of their minor children J.S., B.S., T.S., and B.S., and on behalf of all others similarly situated (collectively, “Class members”), by and through their attorneys, bring this Class Action Complaint against Defendants ESO Solutions, Inc. (“ESO”) and Bon Secours Mercy Health, Inc., d/b/a Mercy Health (“BSMH”) (collectively, “Defendants”), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

**INTRODUCTION**

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their and approximately 2,700,000 other individuals’ personally identifying information (“PII”) and personal health information (“PHI”), including names, dates of birth, injury type, injury date, treatment date, treatment type, and Social Security numbers.

2. BSMH is one of the largest health care systems in the country. It operates healthcare facilities in New York, Ohio, Kentucky, Virginia, Maryland, South Carolina, and Florida, which provide a range of healthcare services. ESO is a third-party vendor of software and data solutions used by BSMH.

3. On or about September 28, 2023, an unauthorized third party gained access to ESO's network system and obtained files containing information about BSMH's and other healthcare companies' current and former patients (the "Data Breach").

4. Defendants owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach, which occurred on or about September 28, 2023.

6. Plaintiffs, on behalf of themselves, their minor children, and all other Class members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Ohio Deceptive Trade Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

**PARTIES**

***Plaintiff Michael Smith***

7. Plaintiff Michael Smith is a citizen of Ohio.

8. Plaintiff Michael Smith obtained healthcare or related services from a BSMH location in Ohio. As a condition of receiving services, BSMH required Plaintiff Michael Smith to provide it with his PII/PHI.

9. Plaintiff Michael Smith also obtained healthcare or related services from BSMH for his minor children J.S., B.S., T.S., and B.S. As a condition of receiving services, BSMH required Plaintiff Michael Smith to provide it with his minor children's PII/PHI.

10. Based on representations made by BSM, Plaintiff Michael Smith believed BSMH had implemented and maintained reasonable security and practices to protect his and his minor children's PII/PHI, including contracting with third-party vendors who would adequately protect his and his minor children's PII/PHI. With this belief in mind, Plaintiff Michael Smith provided his and his minor children's PII/PHI to BSMH in connection with receiving healthcare services provided by BSMH.

11. At all relevant times, Defendants stored and maintained Plaintiff Michael Smith's and his minor children's PII/PHI on their network systems.

12. Plaintiff Michael Smith takes great care to protect his and his minor children's PII/PHI. Had Plaintiff Michael Smith known that BSMH does not adequately protect the PII/PHI in its possession, including by contracting with companies that do not adequately protect the PII/PHI in their possession, he would not have obtained healthcare services from BSMH or agreed to entrust them with his or his minor children's PII/PHI.

13. Plaintiff Michael Smith received a letter notifying him that his PII/PHI was affected in the Data Breach. Additionally, each of his minor children received a letter notifying them that their PII/PHI was affected in the Data Breach.

14. As a direct result of the Data Breach, Plaintiff Michael Smith and his minor children have suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of their highly sensitive PII/PHI; deprivation of the value of their PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Tussie Smith***

15. Plaintiff Tussie Smith is a citizen of Ohio.

16. Plaintiff Tussie Smith obtained healthcare or related services from a BSMH location in Ohio. As a condition of receiving services, BSMH required Plaintiff Tussie Smith to provide it with her PII/PHI.

17. Plaintiff Tussie Smith also obtained healthcare or related services from BSMH for her minor children J.S., B.S., T.S., and B.S. As a condition of receiving services, BSMH required Plaintiff Tussie Smith to provide it with her minor children's PII/PHI

18. Based on representations made by BSMH, Plaintiff Tussie Smith believed BSMH had implemented and maintained reasonable security and practices to protect her and her minor children's PII/PHI, including contracting with third-party vendors who would adequately protect her and her minor children's PII/PHI. With this belief in mind, Plaintiff Tussie Smith provided her and her minor children's PII/PHI to BSMH in connection with receiving healthcare services provided by BSMH.

19. At all relevant times, Defendants stored and maintained Plaintiff Tussie Smith's and her minor children's PII/PHI on their network systems.

20. Plaintiff Tussie Smith takes great care to protect her and her minor children's PII/PHI. Had Plaintiff Tussie Smith known that BSMH does not adequately protect the PII/PHI in its possession, including by contracting with companies that do not adequately protect the PII/PHI in their possession, she would not have obtained healthcare services from BSMH or agreed to entrust them with her or her minor children's PII/PHI.

21. Plaintiff Tussie Smith received a letter notifying her that her PII/PHI was affected in the Data Breach. Additionally, each of her minor children received a letter notifying them that their PII/PHI was affected in the Data Breach

22. As a direct result of the Data Breach, Plaintiff Tussie Smith and her minor children have suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of their highly sensitive PII/PHI; deprivation of the value of their PII/PHI; and overpayment for services that did not include adequate data security.

***Defendant ESO Solutions, Inc.***

23. Defendant ESO Solutions, Inc. is a Texas corporation with its principal place of business at 11500 Alterra Parkway, Suite 100, Austin, Texas 78758-3192. It may be served through its registered agent: C T Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

***Defendant Bon Secours Mercy Health, Inc.***

24. Defendant Bon Secours Mercy Health, Inc. is a Maryland corporation with its headquarters located at 1701 Mercy Health Pl., Cincinnati, OH 45237. BSMH may be served

through its registered agent: Corporation Service Company, 3366 Riverside Drive, Ste. 103, Upper Arlington, OH 43221.

### **JURISDICTION AND VENUE**

25. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

26. This Court has personal jurisdiction over ESO because ESO is a Texas corporation with its principal place of business in this District.

27. This Court has personal jurisdiction over BSMH because BSMH contracted with ESO, which is a Texas corporation, and shared Plaintiffs' PII/PHI with ESO in Texas.

28. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because ESO's principal place of business is located in Travis County, Texas. BSMH provided ESO with the PII/PHI of Plaintiffs in this District, and a substantial part of the events giving rise to Plaintiffs' claims arose in this District.

### **FACTUAL ALLEGATIONS**

#### ***Overview of Defendants***

29. BSMH is one of the largest catholic health systems in the United States.<sup>1</sup> It operates 48 hospitals and has more than 3,000 providers in the United States.<sup>2</sup> Operating as Mercy Health,

---

<sup>1</sup> *Who We Are*, BON SECOURS MERCY HEALTH, <https://bsmhealth.org/who-we-are/> (last accessed Jan. 2, 2024).

<sup>2</sup> *Id.*

BSMH has approximately 35,000 employees across Ohio and Kentucky and offers more than 600 points of care.<sup>3</sup>

30. In the regular course of its business, BSMH collects and maintains the PII/PHI of its current and former patients. BSMH required Plaintiffs and Class members to provide their PII/PHI as a condition of receiving healthcare services from BSMH.

31. BSMH's Mercy Health website states it is "committed to protecting the privacy of medical information we create or receive about you."<sup>4</sup>

32. BSMH's Mercy Health website contains a Notice of Privacy Practices ("Privacy Policy").<sup>5</sup> The Privacy Policy states, "Mercy Health is committed to protecting medical information about you."<sup>6</sup> BSMH acknowledges that it is required by law to "make sure that your medical information is protected."<sup>7</sup>

33. The Privacy Policy describes the ways BSMH can use and disclose its patients' medical information, including for treatment, payment, and healthcare operations.<sup>8</sup> The Privacy Policy requires BSMH to obtain patients' written permission before it can use or disclose medical information for marketing purposes or "to disclose your medical information in exchange for remuneration."<sup>9</sup>

---

<sup>3</sup> *Why Mercy*, MERCY HEALTH, <https://www.mercy.com/about-us> (last accessed Jan. 2, 2024).

<sup>4</sup> *Notice of Privacy Practices*, MERCY HEALTH, <https://www.mercy.com/patient-resources/notice-of-privacy-practices> (last accessed Jan. 2, 2024).

<sup>5</sup> *Notice of Privacy Practices*, MERCY HEALTH, available at <https://www.mercy.com/patient-resources/notice-of-privacy-practices> (download through link titled "English Notice of Privacy Practices") [hereinafter "BSMH Privacy Policy"].

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

34. BSMH's Mercy Health website also states that it will "[p]rotect the patient's right to personal privacy and informational confidentiality in accordance with the law and professional ethics."<sup>10</sup>

35. ESO claims to offer "an integrated suite of software products for EMS agencies, fire departments, and hospitals . . . ." <sup>11</sup> ESO provided services to BSMH, which involved BSMH sharing Plaintiffs' and Class members' PII/PHI with ESO.

36. ESO's website contains an article that states, "In this digital age, keeping personal identification information secure is a priority."<sup>12</sup> The article also notes, "[U]nderstanding and educating staff on current HIPAA requirements is an important and necessary practical reality for organizations."<sup>13</sup>

37. Plaintiffs and Class members are current or former patients of BSMH or other healthcare companies and entrusted BSMH or those other healthcare companies with their PII/PHI.

### ***The Data Breach***

38. On or about September 28, 2023, "an unauthorized third party accessed and encrypted some of ESO's computer systems."<sup>14</sup> Through an investigation into the Data Breach, ESO discovered that "patient information was located on one of the impacted systems."<sup>15</sup>

---

<sup>10</sup> *Mercy Health Patient Rights and Responsibilities*, MERCY HEALTH, <https://www.mercy.com/patient-resources/patient-rights> (last accessed Jan. 2, 2024).

<sup>11</sup> *About ESO*, ESO SOLUTIONS, <https://www.eso.com/about/> (last accessed Jan. 2, 2024).

<sup>12</sup> *HIPAA Compliance and Telehealth*, ESO SOLUTIONS, <https://www.eso.com/blog/hipaa-compliance-and-telehealth/> (last accessed Dec. 22, 2023).

<sup>13</sup> *Id.*

<sup>14</sup> *Notice of Cybersecurity Incident*, ESO Solutions, <https://www.eso.com/notice-of-cybersecurity-incident/> (last accessed Dec. 22, 2023).

<sup>15</sup> *Id.*

39. According to the ESO's letter to the Office of the Maine Attorney General, the PII/PHI affected includes "names, dates of birth, injury type, injury date, treatment date, treatment type and, in some cases, social security numbers."<sup>16</sup>

40. Though ESO learned of the Data Breach on or about September 28, 2023, and learned that PII/PHI was affected in the Data Breach on or about October 23, 2023, it waited until approximately December 12, 2023, almost two months later, to begin notifying Plaintiffs and Class members that their PII/PHI was in the hands of cybercriminals.<sup>17</sup>

41. ESO's failure to promptly notify Plaintiffs and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

***Defendants Knew that Criminals Target PII/PHI***

42. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected and stored was a target for malicious actors. Indeed, ESO's website describes the importance of the safeguarding of PII/PHI.<sup>18</sup>

---

<sup>16</sup> *ESO Solutions, Inc. - Data Security Incident*, OFFICE OF THE MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aviewer/ME/40/bd939a31-70fd-4f7c-99cf-d6b87906489f/3d7d81ef-0260-48c7-93a8-0f8ea1025caf/document.html> (last accessed Dec. 22, 2023).

<sup>17</sup> *See Notice of Cybersecurity Incident*, *supra* note 14.

<sup>18</sup> *See HIPAA Compliance and Telehealth*, *supra* note 12.

43. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyberattacks that Defendants should have anticipated and guarded against.

44. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers (“SSNs”) and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores.”<sup>19</sup>

45. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.<sup>20</sup> This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.<sup>21</sup>

46. PII/PHI is a valuable property right.<sup>22</sup> The value of PII/PHI as a commodity is measurable.<sup>23</sup> “Firms are now able to attain significant market valuations by employing business

---

<sup>19</sup> Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

<sup>20</sup> See PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/breach-barometer-report> (last accessed Jan. 2, 2024).

<sup>21</sup> See *id.*

<sup>22</sup> See Marc van Lieshout, *The Value of Personal Data*, 457 INT’L FED’N FOR INFO. PROCESSING 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . .”), [https://www.researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data).

<sup>23</sup> See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”<sup>24</sup> American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.<sup>25</sup> It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

47. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

48. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”<sup>26</sup> A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”<sup>27</sup>

49. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each

---

<sup>24</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLibrary (April 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en).

<sup>25</sup> See IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

<sup>26</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (“*What Happens to Stolen Healthcare Data*”) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

<sup>27</sup> *Id.*

on the black market.<sup>28</sup> According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.<sup>29</sup>

50. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”<sup>30</sup> Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”<sup>31</sup>

51. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”<sup>32</sup>

---

<sup>28</sup> See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

<sup>29</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

<sup>30</sup> Steager, *supra* note 26.

<sup>31</sup> *Id.*

<sup>32</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

52. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

53. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.<sup>33 34</sup>

54. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.<sup>35</sup>

---

<sup>33</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed Nov. 7, 2023).

<sup>34</sup> The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

<sup>35</sup> See Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

55. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.<sup>36</sup>

56. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

57. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, “If I have your name and your Social Security number and you don’t have a credit freeze yet, you’re easy pickings.”<sup>37</sup>

58. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”<sup>38</sup> It “is also more difficult to detect, taking almost twice as long as normal identity theft.”<sup>39</sup> In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get

---

<sup>36</sup> Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), <https://www.idtheftcenter.org/publication/2023-consumer-impact-report/> (last accessed Nov. 7, 2023).

<sup>37</sup> Patrick Lucas Austin, ‘*It Is Absurd.*’ *Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

<sup>38</sup> Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), [http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF\\_Geography\\_of\\_Medical\\_Identity\\_Theft\\_fs.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).

<sup>39</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 29.

prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”<sup>40</sup> The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to use.”<sup>41</sup>

59. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim’s debt collection and credit problems, through no fault of their own.<sup>42</sup>

---

<sup>40</sup> See *What to Know About Medical Identity Theft*, FED. TRADE COMM’N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Nov. 7, 2023).

<sup>41</sup> *Id.*

<sup>42</sup> See Dixon & Emerson, *supra* note 38.

60. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.<sup>43</sup>

61. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

### ***Damages Sustained by Plaintiffs and Class Members***

62. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

### **CLASS ALLEGATIONS**

63. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

---

<sup>43</sup> John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

64. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

All United States residents whose PII/PHI was accessed by unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

65. Plaintiffs also bring this action on behalf of the following subclass, called the “BSMH Subclass”:

All United States residents who provided their PII/PHI to BSMH and whose PII/PHI was accessed by unauthorized persons in the Data Breach, including all United States residents who provided their PII/PHI to BSMH and were sent a notice of the Data Breach.

66. Excluded from the Class are Bon Secours Mercy Health, and its affiliates, parents, subsidiaries, employees, officers, agents, and directors; ESO Solutions, Inc., and its affiliates, parents, subsidiaries, employees, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge.

67. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

68. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. ESO has reported to the Office of the Maine Attorney General that 2,700,000 persons were affected by the Data Breach.<sup>44</sup>

69. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

---

<sup>44</sup> *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aeviewer/ME/40/bd939a31-70fd-4f7c-99cf-d6b87906489f.shtml> (last accessed Jan. 2, 2024).

- a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;
- b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiffs and Class members to unauthorized third parties;
- c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;
- d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;
- e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiffs and Class members;
- f. Whether Defendants breached their duties to protect Plaintiffs' and Class members' PII/PHI; and
- g. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

70. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

71. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

72. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or

that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

73. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CAUSES OF ACTION**

### **COUNT I NEGLIGENCE**

74. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

75. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

76. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure

systems. Defendants knew or should have known of the many data breaches that targeted healthcare providers that collect and store PII/PHI in recent years.

77. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

78. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

79. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

80. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

81. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in

the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

**COUNT II**  
**NEGLIGENCE PER SE**

82. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

83. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

84. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as BSMH, of failing to employ reasonable measures to protect and secure PII/PHI.

85. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiffs' and other Class members' PII/PHI, by failing to provide timely notice, and

by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

86. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

87. Plaintiffs and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

88. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Breach.

89. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

90. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violations of the HIPAA Privacy and Security Rules, and Section 5 of the FTCA. Plaintiffs and Class members have suffered and will suffer injury,

including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

**COUNT III**  
**BREACH OF FIDUCIARY DUTY**  
*Against BSMH Only on Behalf of the BSMH Subclass*

91. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

92. Plaintiffs brings this claim on behalf of themselves and the BSMH Subclass against only BSMH.

93. Plaintiffs and BSMH Subclass members gave BSMH their PII/PHI in confidence, believing that BSMH would protect that information. Plaintiffs and BSMH Subclass members would not have provided BSMH with this information had they known it would not be adequately protected. BSMH's acceptance and storage of Plaintiffs' and BSMH Subclass members' PII/PHI created a fiduciary relationship between BSMH and Plaintiffs and BSMH Subclass members. In light of this relationship, BSMH must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiffs' and BSMH Subclass Members' PII/PHI.

94. Due to the nature of the relationship between BSMH and Plaintiffs and BSMH Subclass members, Plaintiffs and BSMH Subclass members were entirely reliant upon BSMH to ensure that their PII/PHI was adequately protected. Plaintiffs and Class members had no way of verifying or influencing the nature and extent of BSMH's or its vendors data security policies and practices, and BSMH was in an exclusive position to guard against the Data Breach.

95. BSMH has a fiduciary duty to act for the benefit of Plaintiffs and BSMH Subclass Members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to, properly protect the integrity of the system containing Plaintiffs' and BSMH Subclass members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and BSMH Subclass members' PII/PHI that they collected.

96. As a direct and proximate result of BSMH's breaches of its fiduciary duties, Plaintiffs and BSMH Subclass members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in BSMH's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

**COUNT IV**  
**BREACH OF IMPLIED CONTRACT**  
***Against BSMH Only***

97. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

98. Plaintiffs brings this claim on behalf of themselves and the BSMH Subclass against only BSMH.

99. In connection with receiving healthcare services, Plaintiffs and all other BSMH Subclass members entered into implied contracts with BSMH.

100. Pursuant to these implied contracts, Plaintiffs and BSMH Subclass members paid money to BSMH, directly or through their insurance, and provided BSMH with their PII/PHI. In exchange, BSMH agreed to, among other things, and Plaintiffs and BSMH Subclass members understood that BSMH would: (1) provide services to Plaintiffs and BSMH Subclass members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and BSMH Subclass members' PII/PHI; and (3) protect Plaintiffs' and BSMH Subclass members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

101. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and BSMH Subclass members, on the one hand, and BSMH, on the other hand. Indeed, as set forth *supra*, BSMH recognized the importance of data security and the privacy of BSMH's patients' PII/PHI. Had Plaintiffs and BSMH Subclass members known that BSMH would not adequately protect their PII/PHI, they would not have received healthcare or other services from BSMH.

102. Plaintiffs and BSMH Subclass members performed their obligations under the implied contract when they provided BSMH with their PII/PHI and paid for healthcare or other services from BSMH.

103. BSMH breached its obligations under its implied contracts with Plaintiffs and BSMH Subclass members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, including by ensuring companies it contracts with implement and maintain reasonable security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and BSMH Subclass members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

104. BSMH's breach of its obligations of its implied contracts with Plaintiffs and BSMH Subclass members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

105. Plaintiffs and all other Class members were damaged by BSMH's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

**COUNT V**  
**UNJUST ENRICHMENT**

106. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

107. This claim is pleaded in the alternative to the breach of implied contract claim.

108. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid to BSMH for healthcare services, which BSMH used in turn to pay for ESO's services, and through the provision of their PII/PHI.

109. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Defendants also benefitted from the receipt of Plaintiffs' and Class members' PII/PHI, as this was used to facilitate billing services and services provided to BSMH.

110. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

111. Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

112. Plaintiffs and Class members have no adequate remedy at law.

113. Defendants should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

**COUNT VI**  
**VIOLATIONS OF THE OHIO DECEPTIVE TRADE PRACTICES ACT,**  
**Ohio Rev. Code § 4165.01, *et seq.* (“ODTPA”)**

114. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

115. Plaintiffs and Defendants are each “persons” as defined in the ODTPA.

116. Defendants intentionally represented that their services included adequate data security practices and procedures that would ensure the safety of Plaintiffs’ and Class members’ PII/PHI.

117. Defendants’ services did not include, as advertised. Defendants advertised their services as including adequate data security practices and procedures, when in fact the services did not include adequate data security practices and procedures.

118. Defendants did not intend to supply Plaintiffs and Class members with services that included adequate data security practices and procedures, as advertised.

119. Defendants’ conduct constitutes violations of the ODTPA.

120. Defendants also engaged in unlawful and unfair practices in violation of the ODTPA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Plaintiffs’ and Class members’ PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

121. Defendants make explicit statements to their patients that their PII/PHI will remain private.

122. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII/PHI. Further, Defendants’ failure to adopt, or contracting with companies that failed to adopt, reasonable practices in protecting and safeguarding their patients’ PII/PHI will force

Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

123. As a result of Defendants' violations of the ODTPA, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in BSMH's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

#### **PRAYER FOR RELIEF**

Plaintiffs, individually and on behalf of all other Class members, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

- A. Certifying the Class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;
- B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;
- C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by

adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

**JURY TRIAL DEMANDED**

Plaintiffs demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 2, 2024

Respectfully submitted,

/s/ Bruce W. Steckler

Bruce W. Steckler

State Bar No. 00785039

Austin P. Smith

State Bar No. 24102506

**Steckler Wayne & Love, PLLC**

12720 Hillcrest Road

Dallas, Texas 75230

Tel: (972) 387-4040

Fax: (972) 387-4041

bruce@swclaw.com

austin@swclaw.com

Ben Barnow\*

Anthony L. Parkhill\*

**Barnow and Associates, P.C.**

205 West Randolph Street, Suite 1630

Chicago, IL 60606

Tel: 312-621-2000

Fax: 312-641-5504

b.barnow@barnowlaw.com

aparkhill@barnowlaw.com

*\*pro hac vice forthcoming*